NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: November 2005 **LETTER NO.: 05-CU-18**

TO: Federally Insured Credit Unions

SUBJ: Guidance on Authentication in Internet Banking Environment

ENCL: Federal Financial Institutions Examination Council Authentication in an Internet Banking Environment

DEAR BOARD OF DIRECTORS:

Federally Insured Credit Unions are increasingly offering a variety of Internet banking services ranging from simple inquiry to complex e-Commerce activities for their members. In parallel, the number of members using transactional sites grew significantly. As e-Commerce services increase in volume and complexity, criminals are using more sophisticated methods for account fraud and identity theft. You should become more diligent to safeguard member information, to prevent money laundering and terrorist financing, to reduce fraud, and to inhibit identity theft. One of the effective security measures to mitigate these risks is to implement an effective and reliable authentication system.

Authentication is the process of verifying a member's identity using a variety of methodologies and technologies before the member gains access to the system. It is a way to ensure members are who they say they are. A single-factor authentication such as user name and password used as a security control mechanism may not be adequate for high-risk transactions involving access to member information or fund transfers.

To assist credit unions' efforts in implementing an appropriate authentication system, the NCUA and other Federal Financial Institutions Examination Council (FFIEC) member agencies[1] have developed the enclosed authentication guidance. This

[1] Federal Financial Institution Examination Council member agencies include Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

guidance addresses the need for risk-based assessments, member account authentication, monitoring / reporting, and member awareness about the identity theft using a federally insured credit union's Internet-based services as highlighted below. You should use this guidance when evaluating and implementing authentication systems and practices, whether they are provided internally or through a service provider. Credit unions are expected to have achieved conformance with the guidance by year-end 2006.

Risk Assessment

You should identify and evaluate the risks associated with the Internet related services you provide for your members. This assessment should take into consideration type of member (e.g., member account vs. business account); member transactional capabilities (e.g., share draft vs. bill payment, wire transfer, loan origination); confidentiality of the member information being communicated between the credit union and the member; ease of using of the communication method; volume of transactions.

Ultimately, the risk assessment should result in the implementation of risk mitigation controls and techniques commensurate to the type and level of risks presented by the Internet related services.

Member Account Authentication

Where the risk assessment indicates that the use of single-factor authentication is inadequate for the types of services period, you should employ multifactor authentication[2], layered security[3], or other controls. You should develop an ongoing process to review and implement appropriate authentication technology.

Monitoring and Reporting

You should have policies and procedures in place that adequately monitor the system access. If you detect unauthorized access to applications and members' accounts, report to local law enforcement and your NCUA Regional Director. In addition to the strong authentication, you should consider implementing multiple layers of security controls such as independent audits and logs reviews to assist in the detection of unauthorized activities.

If critical systems or processes are outsourced to a vendor or third party, you should ensure appropriate computer network logging and monitoring procedures are in place at

---

[2] Multifactor authentication uses more than one factor such as ID/Passwords, smartcards, tokens, fingerprints, or retinal scans to authenticate users.

[3] Layered security is segregating public and private networks, deploying overlapping controls for access and asset protection, constructing DMZs and bastion hosts--these and other security techniques help organizations secure their intellectual property and proprietary communications.

the vendor. Any unauthorized activities through a vendor's or third party's system should be reported to you in a timely fashion.

For additional guidance on incident response, please review Appendix B, Part 748 of the NCUA Rules & Regulations.

Member Awareness

Member education is critical in terms of reducing account fraud and identity theft. You should implement a customer awareness program and evaluate current education efforts to determine if additional steps are necessary.

Verification

Examiners will begin to assess progress in meeting the expectations outlined in the guidance. You are expected to achieve full compliance with the guidance by year-end 2006.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/

JoAnn M. Johnson
Chairman

Enclosure